Developing a National Policy on Cyber Security

Michelle Van Cleave
Special Assistant to the Under Secretary for Policy – Department of Defense

CONTENT

INTRODUCTION

The subject that I have been asked to address is that of a national policy for cyber security, so I need to begin with a bit of an introduction and a disclaimer. The introduction is that the work that I am currently doing for the Secretary of Defense is helping to design a new office for Homeland Security within the Office of the Secretary of Defense (OSD). This is something that came to the forefront post September 11 and is of immediate concern. A Northern combatant command will set be up for the purpose of taking on the homeland defense and civil support missions of the armed forces within the United States. We will need to have an equivalent civilian organization within the Secretary's office to be able to provide the staff support that he will require. That is what I have been working on and frankly, we have not been doing much in the way of cyber security at this stage, so that it is both a disadvantage and an opportunity. The disadvantage is that you may or may not be getting the most current perspective from the Department of Defense (DOD) on cyber security from my remarks. On the other hand, since I have no official responsibilities in this area, I can and will speak today not as a representative of the Department of Defense, but as a freewheeling critic. So some of the observations I am about to offer may not sound like they are being presented from Washington, because they are not.

EXISTING NATIONAL POLICY FOR CYBER SECURITY

The national policy for cyber security as it is today, is embodied in a handful of key documents and studies that emerged from work that was done in the 1990's on critical infrastructure protection. I do not know how familiar this audience is with the history of critical infrastructure protection, but let me say that the President's Commission on

Critical Infrastructure Protection compiled a report in this area concluding that we are vulnerable, the threat is growing, it is getting worse, and we are not doing much about it. As a consequence, there was a Presidential Decision Directive (PDD 63), issued relatively late in the Clinton Administration, which established as national policy the objective that we should be doing something about this. The PDD created a couple of offices charged with that responsibility at the FBI National Infrastructure Protection Center and at the Department of Commerce. To support the national level efforts, the Critical Infrastructure Assurance Office and the position of National Coordinator for Critical Infrastructure Protection on the National Security Council (NSC) staff were created. Named to that job was Richard Clarke.

There were also important congressional hearings and other congressional activities of note. These included seminal hearings held by Senator Nunn's sub-committee and studies directed by Senator Kyl. Most recently, we had an executive order issued that is far reaching in this area and looks at other aspects of cyber security in addition to critical infrastructure protection. The principal purpose of this new executive order is to rationalize the various interagency efforts ongoing in different areas of cyber security, which are many and diverse.

The work of the National Security Telecommunications and Information System Security Committee (NSTISSC) has long concentrated on one set of activities. Those activities pertain largely to the security of national security information and associated information systems against intrusion or compromise. The NSTISSC does not look at the terrorist threat per se; its focus is the penetration threat. The National Communications System oversees the telecommunications preparedness of the nation, working through its Committee of Principals composed of representatives of the 22 departments and agencies that are members of the NCS. Its purpose is to ensure enduring national security emergency communications capabilities across the full range of potential crises, from floods and hurricanes to nuclear war. The Chief Information Officers Council (CIO), headed up by the Office of the Management and Budget (OMB), is yet another interagency body looking at the health of the information infrastructure. All of these bodies were brought under a new Board on Cyberspace Security. Richard Clark was named as the Assistant to the President for Cyberspace Security. He left one job to take on another job in a new structure, and the work continues.

We also had a Homeland Security Office created within the White House, as you all know. There is another council, the Homeland Security Council, equivalent to the National Security Council (NSC), which coordinates the work of the various departments and agencies. The White House Office of Homeland Security has not really gotten involved in cyber security threat matters as of yet. However, because their mission is to protect against all terrorist activities in the United States, it certainly falls within its charter. The NSC still has lingering interest in cyber security. An evaluation will have to be made to determine how all these different bodies work together, in terms of their efficiency and efficacy.

I would suggest to you that the bureaucracy is not the only thing that is in need of straightening out at this point. It is my opinion that despite over a decade of work, we still lack the fundamental elements of a national strategy for protecting our critical infrastructures against cyber attacks. It seems to me that we need to define the purpose and substance of this undertaking and then derive policy and bureaucratic implications from there.

VULNERABILITIES OF CRITICAL INFRASTRUCTURES

Concern over the vulnerability of our critical infrastructures emerged with the growing realization that information-based networks, while tremendously enhancing efficiency and power, also imported vulnerabilities. The daily bombardments of these networks by experimenters, hackers, and sinister actors, are something that the critical infrastructures of this country have been facing. The early awareness of these vulnerabilities was not especially government driven or even principally government driven. For instance in the early 1980's, the NSTAC, which is the body of advisors to the President on telecommunications viability, called attention to the growing vulnerability to computer intrusions of the public switch network. However, public discussion about these vulnerabilities was muted due to the concern over the commercial implications of talking too much. Likewise, self-help is no stranger to the banking community in dealing with these kinds of problems. The industries that own and operate the nation's critical infrastructures are of course active in protecting their networks against cyber intrusions.

Government has long understood the permeability of government information systems to the compromise of information. Security measures of this sort have a long history. Ensuring the reliability of infrastructures to support critical government functions has long been a part of national policy. This kind of national policy, National Security Emergency Preparedness, is also embodied in some key documents. Executive Order 12656 from the early Reagan Administration assigned roles and responsibilities for emergency preparedness across all of the departments and agencies. Executive Order 12472 specifically addresses telecommunications preparedness. As a result, planning that grows out of national security emergency preparedness, indicates to us that we have to be prepared so that government can endure any type of national security emergency. The ability of government to endure, reconstitute, and recover is needed in order to provide the essential emergency services that are provided after a fire, flood, attack, nuclear war, or any other type of disaster. The scope of the critical infrastructure protection problem is really one that we need to delineate in order to be able to develop appropriate national policy to answer it.

THREE LEVELS OF CYBERSECURITY CONCERNS

In my view, infrastructure assurance or critical infrastructure protection can be understood as comprising three different strata of protection and reliability concerns:

- At the first level of concern, people rely on daily infrastructure services that can be disrupted by day-to-day hazards. Such incidents can vary in severity and are routinely encountered by the owners and operators of the businesses that provide infrastructure services.

- At the next level, government services rely on infrastructure support in times of national security emergencies. A formal process called National Security Emergency Preparedness (NSEP) planning looks to define the requirements that emerge from that reliability so that the government can continue to do the job that it needs to do to deal with emergencies.

- At the last level, which is something wholly different and new, the prospect of strategic information warfare or strategic infrastructure attack impacts the supreme national interests of the country. This concept of strategic information warfare is an utterly new element in national security planning. It is one of several concerns that are generally identified as a tool of asymmetric warfare and one associated not only with terrorist groups, but also, for the most part, with state actors.

So you can see that critical infrastructure protection, as a policy undertaking is the proverbial elephant as described by the blind men. The national policy implications vary depending on what level we are talking about.

Day to Day Operations

The day-to-day operations of an infrastructure can be impacted by natural disasters, equipment failures, operator error, human negligence, or purposeful criminal acts. The owners and operators of these infrastructures have built in a great deal of resilience, reliability, and redundancy because they are in the business of providing services and they understand that they are subject to these types of disruptions. Because this understanding has been around for a long time, the existing institutions and missions that are supporting the operations of these critical infrastructures are well established and have the ability to deal with these matters without having to think about the creation of new government bureaucracies to address them specifically. There are industry associations, for instance, that develop industry-wide standards for reliability. Then there is the liability insurance industry that emerges with yet its own set of requirements. Law enforcement agencies at the federal, state, and local levels generally bring the necessary experience and authority to deal with criminal matters.

For this category of infrastructure protection, industry is fully capable of making its own cost benefit decisions about the kinds of things that it needs to do in order to stay in business and meet the public safety standards to which it must adhere. Existing relationships with law enforcement are also there. Of course, this is not to suggest that there cannot be substantial improvement in the security and protection at this level or that the government does not have a role to play in raising awareness. Generally, it does have

a role. However, I suggest that we really do not need to have centrally-managed government involvement in directing security standards. The infrastructure owners and operators are the ones that engage in the businesses and have the experience and ability to make these assessments. They need to determine what to do by making the necessary risk management judgments and applying corrective measures. The operation of the market also impact infrastructure reliability. In our free market society, industries will arise to provide better quality software and security and supply the ability to deal with computer intrusions. A great deal can be done without the government having to step in to take charge.

Government Reliance on Infrastructure Support

At the second level, when it comes to National Security Emergency Preparedness (NSEP), a real opportunity exists to have a national level policy for cyber security that really makes sense, folded together with other emergency preparedness concerns. In the past, the federal government has developed careful plans for emergency preparedness, in order to be able to continue to perform key missions across all kinds of crises. During the cold war, there was a fair amount of attention given to this type of planning. The government, working with industry, especially the telecommunications industry, as well as with others such as the energy sector, established specific priorities for specific infrastructure support needed to endure across different kinds of emergencies. Industry was able to respond because industry understood exactly what it was that the government needed to have done. Those priorities were met in a cooperative way, and there was even funding involved, which is also good from industry's perspective. If the NSEP planning methodology were applied to critical infrastructure protection today, analytically we would have top down direction identifying the thin line priorities for the infrastructure support needed to ensure that essential emergency needs can be met, from the federal to the state and local levels.

Strategic Information Warfare

Finally, the area of Strategic Information Warfare is a very different problem from the standpoint of designing a national level policy. A potential attacker would be interested in identifying key nodes in order for the attack to have the greatest effect. The defender needs to understand the interrelationships among the infrastructures, as does the attacker. The potential for cascading failures exists since a failure in one node can lead to failures in others, within or across given infrastructures. National policy needs to undertake risk management at a national level to identify the key nodes and assign scarce resources. A serious approach to protecting against strategic information attack would require a national architecture for indications and warnings for such an attack. Both the traditional outward look of intelligence for indications of an attack as well as an inward look that focuses on the infrastructure information systems themselves, are needed to ascertain and characterize disruptions in those networks.

Again, I think it is critically important that we distinguish what level of cyber protection we are talking about because the roles and responsibilities of government and industry at each level are very different. The requirements for information sharing between government and industry will also vary depending on the level of critical infrastructure protection at issue.

DEVELOPING A NEW NATIONAL POLICY FOR CYBER SECURITY

The current Presidential Decision Directive 63 does not distinguish among these different kinds of cyber security concerns. It refers almost exclusively to the first level of concern, i.e., the day-to-day operations of the various infrastructures. It does not acknowledge the central role of national security and emergency preparedness in cybersecurity policy. It does not address strategic information warfare at all, which may be surprising to those who have not had the opportunity to read Presidential Decision Directive 63. Indeed, PDD 63 does not even mention information warfare although it is the seminal policy guidance in this arena. Because the PDD does not address information warfare, it does not assign responsibility for defense against such an eventuality. It does not refer to the indications and warning problems. This may be the directive's most telling weakness. It does not set up a process to identify what is critical among the various infrastructures at issue. There is no process established for identifying which parts of those infrastructures are critical from our standpoint. Finally, this presidential guidance does emphasize the importance of government industry partnership, which of course is obvious and essential, but it does not really provide any insight into what kind of information needs to be shared or to what ends. In my view, there needs to be sufficient analytic rigor brought to this whole idea of national policy for cyber security in order to be able to explain to industry what is expected of it, as well as to define government's role.

My general prescription is three-fold. First, I believe that industry is fully capable of sharing information among itself about different kinds of cyber threats, incidents, and intrusions; and can set up the necessary information sharing mechanisms just fine. We already have a lot of this type of behavior within different industry sectors because it makes a great deal of sense. The National Infrastructure Protection Center (NIPC), which is housed at the FBI, clearly needs to continue to concentrate in the core area of computer crime, because this is a very serious, pressing, and growing concern. The FBI is contending with a full gamut of criminal concerns, including on-line stalking, child pornography, identify theft, and various kinds of Internet fraud.

Second, we need to reinvigorate National Security and Emergency Preparedness planning from the government perspective. We need to concentrate on how we can ensure, from the standpoint of the federal government working with state and local governments down to first responders, that we are prepared to deal with whatever eventualities may arise. Preparation is essential in order to have the ability to do the job American citizens expect of their government in time of an emergency. This is as true for cyber threats directly against infrastructures as it is for other kinds of terrorism and other national security threats.

Finally, strategic information warfare is a serious national security concern, which has not matured into a strategic defense strategy. This, of course, is a federal government responsibility and the question of from where the threat might emanate is certainly of interest. It would seem (and I think most analyses suggest) that cyber attacks do not have as much appeal to terrorists as do other kinds of instrumentalities they might employ to cause death and destruction and induce terror. At the same time, a sophisticated terrorist organization could well employ cyber-type tools in connection with other kinds of attacks, as Richard Scribner (these proceedings, page XX) was suggesting to us earlier.

Nation states, on the other hand, are a very serious concern, especially when one looks at the advantages to be gained from particular attacks against cyber systems at a time of possible conflict. The experience that we have had in national exercises such as Eligible Receiver in the late 1990's, suggest that adversaries could really cause devastating effects on our ability to project force by the use of cyber attacks against critical government information systems.

With respect to protecting against strategic information warfare, there are promising approaches in two areas:

1. **The counterintelligence dimension.** The adversary's need for intelligence to precede any kind of an effective attack is manifest. It is an intelligence intensive undertaking to be able to map and understand the complexities of a network to gain access. That access could lead to recruitment of insiders needed to gain appropriate access to carry out an attack that would result in a catastrophic failure. If an adversary has to go through this type of intelligence acquisition as a precursor to any kind of an attack, he may then present a pattern or a series of activities that can be discerned. The opportunity is to really concentrate on the counter-intelligence side of this and the ability to characterize the foreign intelligence threat to our infrastructures. To be able to array critical infrastructure techniques against that threat that would interdict, deny, or at least give us a better insight into what a potential adversary would be up against is needed to have a more mature counter intelligence strategy and approach to protect our critical infrastructures.

2. **The prospect that our best defense may be our ability to endure.** The other characteristic that suggests a real opportunity is the extent to which a potential adversary may be deterred from going after critical infrastructures because of their inherent robustness. To launch a strategic attack against United States infrastructures would be a profound decision for any potential adversary to make, and would likely depend on the calculation of just how much harm could be done. The extent of the harm would bear some relationship to the extent to which we could reconstitute and recover from that kind of an attack. This is unlike physical destruction of an infrastructure, where something is blown up and it is then gone

for a substantial period of time. Questions regarding a cyber attack would include:

- How much was taken out?
- How long will it be out?
- How agile is the ability to work around that disruption?

Our planning and preparedness to be able to recover from a cyber attack may, in fact, be the best deterrent to such an attack occurring in the first place.

CONCLUSION

I have tried to outline different analytic approaches to national policy for cyber security for your consideration this afternoon, but as we all know, it is impossible to add enough layers of security to protect against all threats. The real protection against terrorists, cyber terrorists, or terrorists of any type is to go on the offense.

I want to conclude by reminding us all that we are at war. We are engaged in a war that has a strategic purpose and that strategic purpose is to create conditions that make it impossible for terrorists to succeed. We need to employ a full range of tools, to include military capabilities, aimed at disrupting terrorist cells, their support, communications links, logistics, and operations, and denying them safe harbor. What the terrorists rely upon as their strengths — their amorphous nature, diverse cell populations, reliance on Internet communications for connectivity, lack of a fixed location, and their mobility across international borders — must be turned into vulnerabilities. As Secretary Rumsfeld has said many times, it is clear that our task in this strategic undertaking is much broader than simply defeating the Taliban or Al Qaeda. It is to root out global terrorist networks and the governments that sponsor them, not just in Afghanistan, but wherever they are to ensure that they cannot threaten the American people or our way of life. And that is what we are doing, one step at a time.

Earlier, it was suggested that this conference has been markedly lacking in optimism. I am not trying to answer the call for optimism. The thought I would leave you with is not mere optimism, but resolve. It is the resolve of our President; it is the calling of our generation. We will win this war. That is our national policy.

MICHELLE VAN CLEAVE

Michelle Van Cleave is Senior Advisor to the Executive Agent for Homeland Security, Department of Defense. She joined the Defense Department on September 21, 2001 as a consultant to the Undersecretary for Policy. Previously, she was co-founder and President of National Security Concepts, Inc., a Washington D.C. firm specializing in strategic planning and senior level policy analysis for government clients. In the 105th Congress, Ms. Van Cleave was the staff director and chief counsel of the Senate Judiciary Subcommittee on Technology, Terrorism and Government Information, which encompassed legislative and oversight work on counter-terrorism, encryption policy, and Year 2000 concerns. The Subcommittee was also the central forum in the Senate for hearings on critical infrastructure protection and the new threats of information warfare.

Prior to moving to Washington, Ms. Van Cleave was an associate with the Los Angeles law firm of Horvitz and Greines, specializing in appellate advocacy. She holds Master of Arts and Bachelor of Arts degrees in International Relations from the University of Southern California (U.S.C.), and a Juris Doctorate degree from the U.S.C. School of Law. Ms. Van Cleave is a member of the bar associations of the State of California and the District of Columbia.